IX kadencja



KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Spraw Zagranicznych**
(nr 23)
z dnia 13 października 2020 r.

Pełny zapis przebiegu posiedzenia

Komisji Spraw Zagranicznych (nr 23)

13 października 2020 r.

Komisja Spraw Zagranicznych, obradująca pod przewodnictwem posła **Marka Kuchcińskiego (PiS)**, przewodniczącego Komisji, rozpatrzyła:

– informację Ministra Spraw Zagranicznych oraz Ministra Cyfryzacji na temat priorytetów polskiej polityki zagranicznej w kontekście dynamicznych procesów politycznych, geopolitycznych i geoekonomicznych.

W posiedzeniu udział wzięli: **Marek Zagórski** sekretarz stanu w Kancelarii Prezesa Rady Ministrów wraz ze współpracownikami, **Piotr Wawrzyk** sekretarz stanu w Ministerstwie Spraw Zagranicznych wraz ze współpracownikami, **Stefan Kamiński** prezes Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji, **Marian Edward Haliżak** profesor na Wydziale Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego oraz **Agnieszka Maliszewska** sekretarz, dyrektor biura Polskiej Izby Mleka.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Marcin Chorzewski**, **Artur Kucharski** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Marek Kuchciński (PiS):

Witam państwa na posiedzeniu Komisji Spraw Zagranicznych. Otwieram posiedzenie. Witam panie i panów posłów. Witam również przedstawicieli rządu: pana ministra Piotra Wawrzyka – sekretarza stanu w Ministerstwie Spraw Zagranicznych, pana ministra Marka Zagórskiego – sekretarza stanu w Kancelarii Prezesa Rady Ministrów. Witam wszystkich pozostałych gości przybyłych na nasze posiedzenie.

Informuję, że posiedzenie zostało zwołane przez marszałek Sejmu na podstawie art. 198j ust. 2 regulaminu Sejmu i będzie prowadzone z wykorzystaniem środków komunikacji elektronicznej umożliwiających porozumiewanie się na odległość. Informuję również, że zgłoszenia do zabrania głosu w dyskusji przez posłów należy wysyłać pod adres mejlowy ksza@sejm.gov.pl. W celu uczestniczenia w dyskusji należy zalogować się w aplikacji Polycom. Dane dostępowe otrzymali państwo w poczcie elektronicznej. Jednocześnie informuję, że posłowie członkowie Komisji obecni na sali obrad głosują przy użyciu urządzenia do głosowania za pomocą legitymacji poselskiej. Wówczas nie logują się w systemie komunikacji elektronicznej i nie używają tabletów.

W tej chwili sprawdzimy kworum. Proszę członków Komisji o zalogowanie się do systemu do głosowania i naciśnięcie dowolnego przycisku, za, przeciw lub wstrzymuję się, aby potwierdzić obecność. Dziękuję. Informuję, że w posiedzeniu uczestniczy 28 posłów, w związku z tym stwierdzam kworum.

Wysoka Komisjo, posiedzenie Komisji zostało zwołane w trybie art. 152 ust. 2 regulaminu Sejmu na wniosek grupy posłów przekazany do Komisji 22 września 2020 r. Wniosek w imieniu wnioskodawców zgłosił poseł Andrzej Szejna. Zgodnie z wnioskiem tematem posiedzenia jest informacja ministra spraw zagranicznych oraz ministra cyfryzacji na temat priorytetów polskiej polityki zagranicznej w kontekście dynamicznych procesów politycznych, geopolitycznych i geoekonomicznych.

Czy pan poseł Szejna chciałby zabrać głos jako następny? Proszę bardzo.

Poseł Andrzej Szejna (Lewica):

Wysoka Komisjo, panie marszałku, dziękuję za zwołanie Komisji i uwzględnienie wniosku grupy posłów. Posłom, którzy podpisali się pod wnioskiem, serdecznie za te podpisy dziękuję, ponieważ uważam, że w kontekście spraw, które poruszamy, oraz otaczających

nas i dziejących się na naszych oczach procesów globalnych tego typu dyskusje powinny odbywać się na posiedzeniu tej właśnie Komisji. To tu powinna wykuwać się strategia myśli, pewne priorytety realizowane następnie przez rząd.

Pierwszą kwestią, którą chciałbym poruszyć, jest ekonomizacja polityki zagranicznej, która moim zdaniem jest jedną z najważniejszych tendencji w stosunkach międzynarodowych ostatnich trzech dekad. Dla kształtu tej polityki istotne jest zapewnienie klarownego sformułowania celów zarówno w perspektywie krótkiej, jak i długookresowej oraz świadomość, że wiele kwestii, które wcześniej uznawane były za należące do polityki wewnętrznej, obecnie zyskało wymiar międzynarodowy. Rozróżnienie w polityce zagranicznej państwa tego, co polityczne, od tego, co ekonomiczne, zanika lub przestaje być sensowne. Skuteczna polityka zagraniczna wymaga jasno sformułowanych celów i dobrze dobranych instrumentów. Złożone procesy geopolityczne i geoekonomiczne wymagają rewizji nie tylko celów, ale i instrumentów działania.

Bez wątpienia geoekonomia zyskuje na znaczeniu i zastępuje geopolitykę, jednak według innych poglądów podejście geoekonomiczne tylko przekształca geopolitykę. Dyplomacja – niestety polska w stopniu w niejednokrotnie niewystarczającym – staje się reprezentantem gospodarek swoich krajów, aktywnie angażując się w promocję, a w wersji rozwiniętej w walkę o coraz większą przestrzeń geoekonomiczną swojego kraju i gospodarki. Wielkość tej przestrzeni geoekonomicznej zależy od prowadzonej polityki gospodarczej i zagranicznej. Oczywiście decydujące znaczenie mają zasoby państwa, a w szczególności umiejętność ich wykorzystania. Wiemy, jak ważny w kształtowaniu przestrzeni geoekonomicznej jest status państwa na rynku energetycznym. Dla Polski to jeden z priorytetów polityki gospodarczej i zagranicznej, jednak brak jasno określonej polityki energetycznej Polski jest istotnym czynnikiem utrudniającym konieczne procesy dostosowawcze sektora do przyjętej strategii klimatyczno-energetycznej UE.

Drugą bardzo ważną kwestią jest transformacja cyfrowa w Europie i w Polsce oraz potrzeba jej przyspieszenia. Zbudowanie w pełni jednolitego cyfrowego rynku zapewni ramy wewnętrzne pozwalające europejskim przedsiębiorstwom, w tym polskim, na rozwój i ekspansję. W konkluzjach po nadzwyczajnym posiedzeniu 1–2 października 2020 r. Rada Europejska postuluje budowę jednolitego rynku cyfrowego dla całej UE, którego jednym z kluczowych elementów ma być budowa sieci 5G. Rada Europejska zastrzegła, że kwestie cyberbezpieczeństwa związane z tym standardem komunikacyjnym powinny opierać się na unijnym zestawie narzędzi przyjętych 29 stycznia 2020 r., czyli „5G toolbox”. Rada Europejska podkreśliła, że potencjalni dostawcy 5G muszą być poddani ocenie opartej na wspólnych, obiektywnych kryteriach.

Wysoka Komisjo, panie przewodniczący, przechodzę od ogółu do szczegółu – z konkretnymi pytaniami otwartymi do panów ministrów. W kontekście ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych – a zakładam, że projekty te są bardzo dobrze znane i nie wymagają ode mnie żadnego omówienia – postawię tylko pytania. Jak definiujecie panowie interes strategiczny Polski? Czy w kontekście geopolitycznym i geoekonomicznym jest to Unia Europejska, budowa samodzielnej pozycji, czy też bez względu na koszty i ekonomiczną kalkulację inwestowanie również i w tym przypadku w strategiczną – na wielu płaszczyznach zasadnie strategiczną – współpracę ze Stanami Zjednoczonymi?

Czy została przeprowadzona rzetelna analiza geopolitycznych i geoekonomicznych skutków tej ustawy? Czy zasadne jest przewodniczenie Kolegium ds. Cyberbezpieczeństwa przez premiera, skoro każda decyzja kolegium będzie przenoszona od razu na najwyższy poziom przestrzeni dyplomatycznej i politycznej w kontekście geopolitycznym i geoekonomicznym? Dla przykładu, pod osobistym kierunkiem premiera będą analizowane m.in. takie zawarte w ustawie kwestie jak prawodawstwo państwa dostawcy w zakresie ochrony praw człowieka i obywatela czy też zdolność ingerencji państwa spoza UE lub NATO w swobodę gospodarczej działalności dostawcy. Odpowiedzi na te pytania mogą zostać zinterpretowane w sposób negatywny dla międzynarodowych partnerów i będą miały wydźwięk w dyplomacji i polityce międzynarodowej. Niebagatelne znaczenie ma fakt, że odwołanie od decyzji komisji będzie przysługiwać tej samej komisji pod przewodnictwem premiera.

Jakie wnioski resort cyfryzacji, już zresztą nieistniejący, wyciągnął z wdrażanych już rozwiązań i decyzji podjętych przez kraje UE w zakresie transformacji cyfrowej? Chodzi mi o kraje UE i NATO. Pytam szczególnie w kontekście kosztów radykalnych dla budżetu państwa i operatorów rozwiązań, bardziej radykalnych niż w Wielkiej Brytanii. Wymiana infrastruktury to koszty operatorów rzędu miliardów złotych. Jakie potencjalne koszty dla państwa polskiego i firm telekomunikacyjnych wynikają z tej ustawy? Czy zostało to policzone? W jaki sposób potencjalne wykluczenie dostawców, na przykład chińskich czy pochodzących z innych krajów, może wpłynąć na budowę i przyspieszenie budowy 5G? Czy są w tej kwestii jakieś rachunki czy analizy, przewidywania?

Dlaczego w ramach przygotowanego projektu nie zostały przedstawione rzetelne analizy oceniające wpływ przyjęcia przepisów na polsko-chińskie stosunki polityczne i na rozwój eksportu do Chin, gdy problem wykluczenia z przetargu lub pominięcia ofert będzie dotyczył firm z państw członków UE i NATO? Przecież decyzja będzie podejmowana na bardzo wysokim szczeblu. Mam tu na myśli pana premiera.

Jaka jest prognoza uruchomienia sieci 5G w obecnej sytuacji opóźnienia i szczególnych kontrowersji prawnych i międzynarodowych, które na pewno nastąpią? Właśnie o nich zresztą dyskutujemy. Czy została przeprowadzona analiza tego, na ile zaproponowane przez Ministerstwo Cyfryzacji regulacje będą zgodne z przepisami UE przy zastosowaniu przepisów umożliwiających wykluczenie podmiotów ze względu na kraj pochodzenia? Czy takie działanie nie zostanie uznane za dyskryminujące podmioty już dopuszczone do działania na wspólnym rynku oraz produkty, które są powszechnie dostępne? Może to skutkować skargami czy postawieniem Polski przed sądem arbitrażowym. Przykład Estonii zapewne jest panom ministrom znany.

Wysoka Komisjo, panie przewodniczący, w naszym posiedzeniu uczestniczą również eksperci, którzy mają na ten temat dużo do powiedzenia. Nie będę więc wchodził w szczegółowe kwestie. Chcę tylko podkreślić, że w dobie ekonomizacji, globalizacji i geoekonomii, która z założenia wypiera polityki geopolityczne, mam nadzieję, że dzisiejsza decyzja i jasne priorytety polityki zagranicznej polskiego rządu, której jednym z głównych celów powinna być dbałość o interes gospodarczy kraju, o rozwój społeczeństwa informatycznego i informacyjnego, są początkiem rzetelnej wymiany zdań, ale też jasnej i klarownej strategii zrozumiałej nie tylko dla nas, posłów, reprezentantów narodu, ale także dla poszczególnych obywateli. Dziękuję.

Przewodniczący poseł Marek Kuchciński (PiS):

Dziękuję panu posłowi. W tej chwili o głos chciałbym prosić panów ministrów. Pan minister Piotr Wawrzyk pierwszy. Proszę bardzo.

Sekretarz stanu w Ministerstwie Spraw Zagranicznych Piotr Wawrzyk:

Dziękuję bardzo. Panie przewodniczący, Wysoka Komisjo, pozwólcie państwo, że w ramach stosowania środków bezpieczeństwa swoje wystąpienie wygłoszę w maseczce. Wiem, że to będzie utrudnienie, ale wydaje mi się, że powinniśmy przestrzegać zasad także na posiedzeniach Komisji.

Panie przewodniczący, Wysoka Komisjo, powszechnie uważa się, że w obecnej chwili stoimy przez przełomowymi wydarzeniami w zakresie rozwoju technologicznego na świecie. Prowadzone w wielu ośrodkach na świecie intensywne prace nad nowymi technologiami w najbliższym czasie doprowadzą zapewne do skokowego rozwoju gospodarek w wielu dziedzinach, takich jak mobilność i transport, inteligentne miasta, rolnictwo, media i rozrywka, ale także zdrowie, przemysł 4.0, administracja publiczna i e-państwo, logistyka, handel czy energetyka. Rozwijane różnego rodzaju nowe technologie w takich obszarach jak robotyzacja, internet rzeczy, sztuczna inteligencja, praktyczne zastosowania fizyki kwantowej, komputery nowej generacji, druki 3D i szereg innych mogą skumulować, owocując nie stopniowymi, ale skokowymi zmianami o znaczeniu dalece przekraczającym rewolucję przemysłową XIX w., nie tylko w zakresie wzrostu gospodarczego, ale też w zakresie organizacji pracy i życia całych społeczeństw i państw.

Warunkiem praktycznego wdrażania technologii o przełomowym charakterze i ich integracji oraz pełnego wykorzystywania ich potencjału jest jednak zapewnienie niezwykle szybkiej, stabilnej i bezpiecznej transmisji danych cyfrowych. Stąd potrzeba rozwoju

łączności komórkowych nowej generacji, takich jak 5G, a nawet 6G. Trzeba to jednak widzieć nie tylko jako usprawnienie w życiu indywidualnych osób, ale także jako budowę układu nerwowego całej przyszłej gospodarki, organizacji instytucji publicznych i państwowych czy codziennego funkcjonowania wielu aspektów naszego życia.

Ocenia się, że dzięki sieci 5G generacja światowej gospodarki może powiększyć się o rząd wielkości odpowiadającej całej gospodarce Indii, której wartość wynosi 2,8 biliona dolarów. Dostępne szacunki dla Polski wskazują, że w wyniku wdrożenia sieci 5G polskie PKB zwiększy się do 2028 r. o ponad 63 mld zł, a liczba miejsc pracy może wzrosnąć o blisko 100 tys.

W tym kontekście nie powinno dziwić, że rozwój nowych technologii, w tym przede wszystkim łączności 5G, z jednej strony w sposób konieczny musi być przedmiotem międzynarodowej współpracy, gdyż żadne państwo nie ma dziś zasobów technicznych i finansowych, żeby takiej rewolucji dokonywać samemu, a z drugiej strony element ten stał się obszarem rywalizacji między czołowymi potęgami świata, która z czasem będzie nabierała również charakteru otwartej konfrontacji. Ten, kto zostanie liderem tego procesu, będzie mógł utrzymywać i zwiększać przewagę technologiczną i przemysłową, a w rezultacie zdobywać wiodącą rolę ekonomiczną, polityczną i militarną na świecie.

Z tego punktu widzenia geopolityczny układ świata podlega procesowi przewartościowań i zmian. Naszym zadaniem jest wytyczenie drogi, która w najlepszy sposób służy interesom państwa polskiego, społeczeństwa, przedsiębiorców, ale też indywidualnych obywateli. W dynamicznie zmieniającym się otoczeniu interes Polski musi być analizowany, weryfikowany i definiowany praktycznie non stop. Decyzje oparte o ten interes muszą bowiem uwzględniać nasze zobowiązania, ale też bilans zysków i strat, a strategia komunikacyjna wobec partnerów zewnętrznych winna jasno stawiać polskie oczekiwania, w tym uwzględnienie polskich interesów oraz korzyści w przypadku uwzględniania tychże interesów, ale też interesów naszych partnerów.

W odniesieniu do łączności 5G czy szerzej – nowych przełomowych technologii interesy Polski muszą obejmować kwestie bezpieczeństwa, szybkiego i efektywnego wdrażania tych technologii oraz w miarę możliwości udziału polskich podmiotów, ich rozwijania i komercjalizacji. Zwracam jednak uwagę na to, że trwająca pandemia COVID-19 uwypukliła zagrożenia płynące z cyberprzestrzeni, a tym samym w istotny sposób znaczenie cyberbezpieczeństwa, a szerzej – kluczową wagę bezpieczeństwa technologicznego, a także bezpieczeństwa łańcucha dostaw wielu dóbr.

Bezpieczeństwo technologiczne jest kluczowym wymiarem bezpieczeństwa narodowego. Bezpieczeństwo infrastruktury komunikacyjnej musi obejmować brak uzależnienia od jednego dostawcy, bezpieczeństwo całego łańcucha dostaw, podwyższenie cyberodporności na potencjalne ataki i zagrożenia, a w końcu bezpieczeństwo samych danych, od którego zależy przecież funkcjonowanie całej infrastruktury krytycznej państwa czy ochrona prywatności informacji przedsiębiorców i obywateli. Dlatego też budowa nowych sieci łączności musi opierać się na zróżnicowaniu dostawców, którzy niezależnie od kraju pochodzenia będą spełniać wysokie rygory techniczne oraz cieszyć się powszechnym zaufaniem i nie będą zagrożeni bojkotem czy ograniczeniami w dostawach ze strony naszych partnerów w zakresie bezpieczeństwa i współpracy gospodarczej.

Polska dąży zatem do wypracowania transparentnych standardów zastosowania nowoczesnych technologii m.in. w oparciu o obiektywne kryteria techniczne, a także jasne zasady etyczne. Jesteśmy przy tym otwarci na współpracę ze wszystkimi partnerami, którzy zasady te zaakceptują i spełnią określone kryteria i wymagania. Jak rozumiem, więcej szczegółów na temat tych mechanizmów przedstawi pan minister.

Kwestie cyberbezpieczeństwa są ważnym elementem relacji dwustronnych Polski oraz naszych działań w ramach Unii Europejskiej oraz Paktu Północnoatlantyckiego, ale także naszej aktywności na forach innych organizacji międzynarodowych, takich jak Organizacja Narodów Zjednoczonych czy Organizacja Bezpieczeństwa i Współpracy w Europie. W relacjach ze Stanami Zjednoczonymi prowadzimy stały i wszechstronny dialog w tematach bezpieczeństwa technologicznego, a także technologii 5G, zarówno w płaszczyźnie dwustronnej, jak i wielostronnej.

Robimy to nie tylko w ramach NATO. Wspólnie uczestniczymy w wymianie poglądów na temat wypracowania wspólnego podejścia do zapewnienia bezpiecznego łańcucha dostaw sprzętu, oprogramowania i usług niezbędnych do wdrożenia sprawnej i bezpiecznej sieci 5G, jaką prowadzi ponad trzydzieści wiodących w tym obszarze państw UE, NATO, ale też państw partnerskich takich jak Australia, Japonia czy Republika Korei. Jedną z płaszczyzn tego dialogu są konferencje na temat bezpieczeństwa technologii 5G w Pradze, które odbyły się w maju ubiegłego roku i we wrześniu tego roku.

W płaszczyźnie bilateralnej wyrazem naszego dialogu ze Stanami Zjednoczonymi było podpisanie przez pana premiera Mateusza Morawieckiego i sekretarza stanu USA Mike'a Pompeo we wrześniu ubiegłego roku polsko-amerykańskiej deklaracji o współpracy w obszarze bezpieczeństwa sieci 5G, która sprzyja w wymianie informacji dotyczących ryzyka związanego z tą technologią oraz intensyfikacji współpracy technicznej. Z uwagą odnotowaliśmy ogłoszenie przez Stany Zjednoczone najpierw inicjatywy 5G Clean Path, a we wrześniu tego roku jej rozszerzonej wersji, 5G Clean Network. Popieramy te z proponowanych tam działań, które mają na celu stworzenie sieci 5G w oparciu o wszystkie wspomniane powyżej wymogi bezpieczeństwa.

Prowadzimy jednak przy tym dialog także z Chinami, najszybciej rozwijającą się dużą gospodarką świata i dostawcą wielu zaawansowanych technologii, także w obszarze technologii 5G. Z uwagą śledzimy chińskie inicjatywy w tym obszarze, takie jak ogłoszona we wrześniu tego roku globalna inicjatywa dotycząca bezpieczeństwa danych. Wobec chińskich partnerów niezmiennie podkreślamy, że wszyscy dostawcy sieci 5G w Polsce niezależnie od kraju ich pochodzenia będą musieli spełnić te same wymagania i kryteria, które zostaną ujęte w zgodnych z przyjętymi zaleceniami UE krajowych regulacjach. Mam nadzieję, że jest to odpowiedź na zgłaszaną przez pana posła wątpliwość.

Takie podejście wpisuje się w istniejące albo planowane działania innych państw europejskich. W budowie systemu 5G Polska nie zamierza nikogo dyskryminować, wykluczać ani stosować podwójnych standardów. Wierzymy, że nasze relacje z Chinami opierają się na realnych możliwościach rozwoju i wzajemnie korzystnej współpracy w wielu obszarach gospodarki.

W naszym przekonaniu nie powinniśmy tracić szansy skorzystania z tych możliwości, ograniczając dialog tylko do jednego aspektu, czyli technologii 5G. W sposób oczywisty technologie 5G stały się ważnym elementem analiz i dyskusji nad zapewnieniem bezpieczeństwa, odporności i interoperacyjności systemów komunikacyjnych Paktu Północnoatlantyckiego, a szerzej – analiz i prac nad wzmocnieniem całościowych systemów cyberbezpieczeństwa sojuszu. W dyskusjach tych Polska także aktywnie zabiera głos, podkreślając konieczność zachowania spójności i zgodności działań prowadzonych w obrębie NATO i UE. UE jest bowiem głównym ośrodkiem analiz i prac mających na celu zapewnienie bezpieczeństwa oraz pełnej kompatybilności łączności sieci 5G w państwach członkowskich, która będzie krwiobiegiem antycypowanego skokowego rozwoju technologicznego i wzrostu gospodarczego Europy, w tym więc także Polski, o czym wspominałem na początku.

Pandemia COVID-19 pokazała, jak ważne na poziomie całego systemu gospodarczego Europy jest zapewnienie względnie wysokiej samowystarczalności i autonomiczności całych sektorów kluczowych dla funkcjonowania państw i społeczeństw. W wielu obszarach nie jest to proste do osiągnięcia, ale doświadczenia tego roku pokazują, że nie negując otwartości gospodarczej UE oraz zasad wolnego handlu, podjęcie dążeń do rozwoju poziomu niezależności od jakichkolwiek dostawców zewnętrznych jest kierunkiem pożądanym. Żadne państwo na świecie takiej samowystarczalności nie jest w stanie dziś sobie zapewnić, ale poziom integrowania gospodarek europejskich skłania do myślenia, że już na poziomie UE w okresie średnim i długoterminowym możliwe będzie poprawienie naszej sytuacji w tym zakresie w najważniejszych dla dalszego rozwoju obszarach nowoczesnych technologii i komunikacji.

Jak wspomniałem wyżej, dziś technologie 5G są w stanie rozwijać Chiny, Korea Południowa, częściowo Japonia i częściowo Europa, a konkretnie dwie firmy europejskie. Dlatego współpraca na poziomie europejskim jest kluczowa dla przyspieszenia zwiększania stopnia niezależności i przyspieszenia rozwoju gospodarczego Europy.

We współpracy winno się znaleźć miejsce także dla polskich firm, które nierzadko wypracowują innowacyjne, ciekawe rozwiązania, ale często brak im finansów i doświadczenia dla przeprowadzenia udanej komercjalizacji swoich pomysłów i dla skalowania umożliwiającego międzynarodowy sukces. Rozwój technologii 5G otwiera pewne możliwości w tym zakresie. Polska administracja i polskie firmy promują rozwiązania umożliwiające wykorzystanie europejskich instrumentów wsparcia. Nie jest zatem tak, jak było to sugerowane w wystąpieniu pana posła, że mamy wybór między współpracą w tym zakresie ze Stanami Zjednoczonymi a współpracą z UE. Te dwa komponenty uzupełniają się, nie są ze sobą sprzeczne, a nawet pożądane jest ich równoległe prowadzenie.

Jednocześnie ważne jest, aby rozwój technologii komunikacyjnych w Europie nie odbywał się w sprzeczności czy w oderwaniu od prac prowadzonych po obu stronach Atlantyku. Polska musi aktywnie uczestniczyć w tych procesach po obu stronach Oceanu Atlantyckiego. Oceniamy, że w długookresowej perspektywie zbieżności te będą coraz większe, relacje transatlantyckie są bowiem oparte na solidnych podstawach zbieżności narodowych interesów bezpieczeństwa państw po obu stronach Atlantyku. Bezpieczeństwo i odporność sieci telekomunikacyjnych ma dla nas i dla innych państw UE, ale też Stanów Zjednoczonych i NATO kluczowe znaczenie.

Właśnie na poziomie UE na dziś najbardziej zaawansowane są prace nad zapewnieniem spójności i wszechstronności standardów bezpieczeństwa sieci 5G. Wynika to z wdrażania na krajowym poziomie zaleceń oraz standardów wskazanych w dokumencie, o którym powiedział przed chwilą pan poseł, czy w zestawie narzędzi przygotowanych przez Komisję Europejską oraz Agencję Unii Europejskiej ds. Cyberbezpieczeństwa przy aktywnym udziale państw, w tym Polski.

Ogłoszony w styczniu 2020 r. unijny zestaw narzędzi określa minimalny poziom harmonizacji rozwiązań w zakresie cyberbezpieczeństwa sieci 5G, które państwa europejskie następnie wdrażają do swoich regulacji krajowych. Kluczowe znaczenie dla sprawnego wdrażania zaleceń dotyczących sieci 5G zostało mocno zaakcentowanie w konkluzjach Rady Europejskiej z października tego roku. Działania takie podejmowane są w szeregu państw europejskich, na przykład we Francji i w Niemczech, ale także w Polsce, gdzie kończą się prace nad nowelizac2ją ustawy o krajowym systemie cyberbezpieczeństwa. Jak rozumiem, więcej informacji również na ten temat przedstawi pan minister.

Na koniec chciałbym dodać, że Ministerstwo Spraw Zagranicznych aktywnie uczestniczy w działaniach na forach innych organizacji międzynarodowych, czyli ONZ i OBWE. Działania te z jednej strony służą zwiększeniu bezpieczeństwa narodowego w cyberprzestrzeni poprzez skupienie wysiłków na implementacji praktycznych wdrożeń prawa międzynarodowego i poprawieniu środków budowy zaufania, a z drugiej strony starają się przeciwdziałać próbom wykorzystywania tych form do prowadzenia i promowania działań sprzecznych z interesami Polski, UE i Paktu Północnoatlantyckiego. Dziękuję bardzo.

Przewodniczący poseł Marek Kuchciński (PiS):

Dziękuję panu ministrowi. W tej chwili proszę o zabranie głosu pana Marka Zagórskiego, ministra cyfryzacji.

Sekretarz stanu w Kancelarii Prezesa Rady Ministrów Marek Zagórski:

Panie przewodniczący, Wysoka Komisjo, szanowni państwo, nawiązując do wystąpienia pana ministra Wawrzyka, postaram się skupić na aspektach bezpośrednio związanych z zakresem cyberbezpieczeństwa w kontekście sieci 5G. Zacznę natomiast od tego, co było punktem wyjścia do zwołania posiedzenia Komisji, czyli od ustawy o krajowym systemie cyberbezpieczeństwa. W kilku zdaniach powiem o powodach dokonania nowelizacji tej ustawy.

Po pierwsze, mamy kontekst krajowy. Na poziomie krajowym mamy dwuletnie doświadczenie funkcjonowania tej ustawy. Jest to czas, w którym postanowiliśmy dokonać pewnych weryfikacji, takich jak m.in. rozbudowanie tego systemu o CSIRT-y sektorowe, włączenie do systemu obowiązkowych elementów security operations center, ale także cały szereg elementów, w tym implementowanie zaleceń związanych z wdra-

żaniem 5G czy szerzej – prawa europejskiego wynikającego z wdrożenia Europejskiego kodeksu łączności elektronicznej.

Jedną z najważniejszych zmian w tym zakresie jest oczywiście wdrożenie mechanizmu oceny dostawców i oceny sprzętu pod kątem cyberbezpieczeństwa. Dzisiaj mamy bowiem stan, w którym nie mamy praktycznie żadnego instrumentu poza dosyć miękkimi rekomendacjami pełnomocnika rządu ds. cyberbezpieczeństwa w zakresie wskazywania oprogramowania sprzętu, które może stanowić potencjalne ryzyko dla bezpieczeństwa integralności sieci telekomunikacyjnych, teleinformatycznych. Chyba nikt na tej sali ani nikt na świecie dziś nie zaprzeczy, że bezpieczeństwo funkcjonowania tych sieci jest jednym z warunków mówienia o bezpieczeństwie państwa i w ogóle o bezpieczeństwie obywateli.

Oprócz wszystkich elementów bezpieczeństwa, do których jesteśmy przyzwyczajeni, czyli bezpieczeństwa realizowanego chociażby przez armię, ministra obrony narodowej, ale także przez infrastrukturę krytyczną, do zestawu środków całego systemu bezpieczeństwa państwa bezwzględnie musimy włączyć także cyberbezpieczeństwo, a w związku z tym takie kluczowe elementy, jakimi obecnie są sieci informatyczne. Stąd także na poziomie unijnym pojawiła się potrzeba oceny dostawców i komponentów wykorzystywanych do budowy sieci teleinformatycznych. O tym będę jeszcze szerzej mówił.

Zwracam uwagę na rozróżnienie, które być może nie wszyscy państwo widzicie. Warto wspomnieć o tym, że są dwa równoległe działania, które musimy wykonać. Musimy to zrobić zarówno z konieczności zapewnienia naszego własnego bezpieczeństwa, ale także biorąc pod uwagę zalecenia Komisji Europejskiej. Z jednej strony mowa jest bowiem o dostawcach, zwracam uwagę – dostawcach, czyli o podmiotach, których potencjalny wpływ na bezpieczeństwo w sieci systemów trzeba przeanalizować. Z drugiej strony mowa jest o konkretnym sprzęcie i oprogramowaniu. Nie przez przypadek te dwa elementy są rozróżnione. Inaczej podejmuje się decyzje odnoszące się do konkretnego oprogramowania i konkretnego sprzętu, a inaczej odnoszące się do dostawcy. Inaczej oceniamy zbiór narzędzi, a inne kryteria muszą zostać zastosowane w ocenie dostawcy.

Projekt ustawy przewiduje dwa mechanizmy. Z jednej strony jest ocena dostawców, której to oceny zgodnie z naszą propozycją będzie dokonywało Kolegium ds. Cyberbezpieczeństwa. Na wniosek członka kolegium, oczywiście przy wsparciu odpowiednich służb i instytucji, będzie badało i określało poziomy ryzyka, które zdefiniowaliśmy cztery, od wysokiego, przez umiarkowane i niskie ryzyko, aż do braku zidentyfikowanego ryzyka. W zależności od tego, jak to ryzyko zostanie ocenione, takie zastosowane będą odpowiednie środki.

Drugi zestaw narzędzi to narzędzia, którymi dysponować będzie pełnomocnik rządu ds. cyberbezpieczeństwa, polegające na kierowaniu ostrzeżeń bądź poleceń zabezpieczających w odniesieniu do konkretnego rodzaju oprogramowania czy konkretnego sprzętu, niezależnie od tego, czy ten sprzęt i to oprogramowanie są wyprodukowane lub dostarczane przez dostawcę, który wcześniej tej ocenie był poddany. Są to dwa procesy, które mogą być ze sobą powiązane, ale wcale nie muszą.

Jak powiedziałem – i o tym mówił pan minister Wawrzyk – to wszystko pojawia się w kontekście relacji, prac w UE i zobowiązań Rzeczypospolitej Polskiej, dlatego że zaproponowane rozwiązania wynikają nie tylko z analizy i oceny funkcjonowania krajowego systemu cyberbezpieczeństwa, ale także z analizy najlepszych rozwiązań stosowanych przez inne państwa UE. Istotne jest podkreślenie, że projekt tworzy możliwości ochrony wrażliwej i krytycznej z punktu widzenia państwa infrastruktury, w tym zwłaszcza teleinformatycznej. Z całą pewnością jednak kontekst sieci nowej generacji był impulsem do podejmowania wszystkich działań w zakresie bezpieczeństwa nie tylko przez Polskę, ale co warte podkreślenia, przez wiele państw, w tym oczywiście państw UE.

Jednym z priorytetów Komisji Europejskiej jest bowiem cyberbezpieczeństwo sieci telekomunikacyjnych. Jak już powiedziałem, znalazło to swoje odzwierciedlenie chociażby w przepisach Europejskiego kodeksu łączności elektronicznej, który zastąpił tzw. dyrektywę ramową. Poza tym, o czym już była mowa, KE zobligowała wszystkie państwa członkowskie do wdrożenia do 2025 r. technologii 5G na obszarach miejskich oraz wzdłuż głównych ciągów telekomunikacyjnych, ale także przede wszystkim wprost

poinformowała wszystkie państwa członkowskie, że ich obowiązkiem jest zapewnienie bezpieczeństwa szerokopasmowej sieci łączności nowej generacji.

Podstawą do zharmonizowania działań na szczeblu europejskim są zalecenia KE z 26 marca 2019 r. w sprawie cyberbezpieczeństwa sieci 5G. Dokument ten stanowi swego rodzaju mapę drogową w procesie ograniczania zagrożeń związanych z wprowadzaniem technologii 5G.

Zalecenia KE aktywizowały państwa członkowskie do zintensyfikowania wysiłków w celu wdrożenia środków bezpieczeństwa. W ramach Grupy Współpracy NIS powstał ekspercki zespół zajmujący się wyłącznie bezpieczeństwem technologii 5G. Państwa dokonały kompleksowych analiz ryzyka w kontekście wdrażania technologii 5G. Efektem tego jest skonsolidowany przez KE raport opublikowany 9 października 2019 r. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa we współpracy z KE i państwami członkowskimi dokonała identyfikacji zagrożeń na poziomie UE. W efekcie tego powstał dokument o nazwie „ENISA threat landscape for 5G networks".

Kolejnym ważnym elementem kształtowania wspólnego europejskiego podejścia do cyberbezpieczeństwa był „5G toolbox", opublikowany w styczniu 2020 r. We wszystkich tych pracach Polska od samego początku aktywnie uczestniczy, w wielu przypadkach jest liderem wprowadzania tych zmian. W związku z tym nasze działania i decyzje na pewno nie odbywają się w oderwaniu do tego, co na tym poziomie dzieje się na w UE. Sygnalizował to już minister Wawrzyk.

Jeśli chodzi o konkluzje Rady Europejskiej z 12 grudnia 2019 r. w sprawie znaczenia 5G dla gospodarki europejskiej oraz potrzeby ograniczania zagrożeń dla bezpieczeństwa związanych z 5G, podkreślono w nich znaczenie zapewnienia ochrony całego cyklu życia technologii 5G, tak aby objąć cały łańcuch dostaw i wszystkie odpowiednie urządzenia. Wskazano na konieczność wypracowania wspólnych norm i środków bezpieczeństwa dla wszystkich producentów, operatorów i dostawców usług i sprzętu, a także na to, że należy zadbać, aby kluczowe elementy, takie jak elementy mające krytyczne znaczenie dla bezpieczeństwa narodowego, pochodziły wyłącznie od wiarygodnych dostawców.

Chcę powiedzieć, że pojęcie „dostawcy wysokiego ryzyka" nie jest pojęciem, które pojawia się w naszej ustawie nagle. Jest to pojęcie, które zostało wypracowane na poziomie KE. Znalezienie możliwości zabezpieczenia się przed wpływem tego typu dostawców na ograniczenie bezpieczeństwa sieci jest jednym z celów wszystkich działań, o których tu mówimy.

Jest też wreszcie wspomniany już tutaj „5G toolbox", czyli zestaw środków dotyczących – podkreślam to bardzo wyraźnie – minimalnej harmonizacji i standaryzacji rozwiązań cyberbezpieczeństwa sieci 5G na poziomie UE. Państwa członkowskie są zobowiązane wprowadzić to na poziomie minimalnym. Mogą to oczywiście rozszerzać. Czego dotyczy „5G toolbox"? Jakie tam są zalecenia? Jest to zaostrzenie wymagań w zakresie bezpieczeństwa infrastruktury i usług telekomunikacyjnych, wprowadzenie oceny profili ryzyka dostawców, czyli to, co wprowadzamy w tym projekcie, czyli stosowanie odpowiednich ograniczeń w odniesieniu do dostawców stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń w odniesieniu do kluczowych zasobów uznanych za krytyczne i wrażliwe.

W ramach Grupy Współpracy NIS z inicjatywy Niemiec i Polski – podkreślam, że współpraca ta ma także charakter bilateralny – powstała ekspercka podgrupa, której celem jest wypracowanie wspólnych, europejskich w tym rozumieniu, standardów cyberbezpieczeństwa dla sieci 5G w ramach wszystkich działań podejmowanych na poziomie UE. Była też mowa o tym, że kluczowe znaczenie dla sprawnego wdrażania „5G toolbox" zostało mocno zaakcentowane w konkluzjach Rady Europejskiej w dniach 1–2 października tego roku. Wyraźnie wskazano, że należy przyspieszyć wdrażanie technologii 5G, a także podkreślono konieczność szybkiej implementacji w państwach zalecenia z „5G toolbox" dotyczącego wdrożenia ograniczeń dla dostawców wysokiego ryzyka. Dostawcy wysokiego ryzyka pojawiają się we wszystkich zaleceniach KE od samego początku. Polska w tych pracach cały czas uczestniczy.

Pan minister Wawrzyk mówił o konferencji praskiej. Kontekst procesu praskiego też jest istotny. Zgromadziło się tam ponad trzydzieści państw, nie tylko z UE, ale także

Australia, Japonia, państwa NATO. Podkreślono tam, co też jest ważne, krytyczne znaczenie bezpiecznego łańcucha dostaw w kontekście bezpieczeństwa państwa i gospodarki. Wskazano na konieczność oceny ryzyka dostawców z państw trzecich, biorąc pod uwagę m.in. model zarządzania, fakt, czy są podpisane porozumienia o współpracy w obszarze bezpieczeństwa, czy zapewnione są najwyższe standardy, chociażby standardy ochrony danych osobowych.

Co więcej, oceny bezpieczeństwa ryzyka dostawców powinny uwzględniać także takie aspekty jak praworządność, środowisko bezpieczeństwa, nadużycia dostawców oraz zgodność z otwartymi, bezpiecznymi standardami. Jednym z efektów konferencji w Pradze dotyczącej bezpieczeństwa było m.in. wspominane już przez pana ministra Wawrzyka porozumienie podpisane 2 września 2019 r. przez premiera Mateusza Morawieckiego oraz sekretarza stanu Mike'a Pompeo pomiędzy Polską a Stanami Zjednoczonymi. Jest to deklaracja o współpracy w obszarze bezpieczeństwa sieci 5G.

Znowu odwołując się do zapisów – oba państwa zdecydowały, że powinno się dokonywać starannej oceny dostawców, biorąc pod uwagę m.in. fakt, czy dany dostawca jest kontrolowany przez obcy rząd, czy ma transparentną strukturę właścicielską oraz czy ma udokumentowane doświadczenie w zakresie etyki korporacyjnej i jest podmiotem podlegającym systemowi prawnemu, w którym wymagana jest transparentność.

Wspominam o tym dlatego, że w przestrzeni publicznej pojawiają się zarzuty, że projekt ustawy jest oderwany od kontekstu polityki zagranicznej i polityki bezpieczeństwa państwa polskiego, a co więcej, że wyrwany jest z kontekstu polityki UE. Chcę więc jasno i wyraźnie powiedzieć, że cały dokument zbudowany jest w oparciu o zalecenia wynikające z tego, co jest wypracowane na poziomie KE i UE, ale także jest elementem całego procesu podejmowania decyzji i współpracy z naszymi partnerami i sojusznikami. Chcę powiedzieć też, że deklaracje o współpracy, dokładnie o takiej samej treści, oprócz Polski podpisały także inne państwa UE i NATO, m.in. Estonia, Rumunia, Czechy i Słowenia.

W wystąpieniu pana posła Szejny była mowa o tym, że sposób zbudowania mechanizmu oceny naraża nas na strategiczne ryzyko w związku z tym, że w ostateczności decyzję o wykluczeniu dostawcy będzie podejmowało tak wysokie gremium. Trzeba powiedzieć, że po pierwsze, rzeczywiście są to decyzje o charakterze strategicznym. Trudno wyobrazić sobie, by tego typu decyzje miały charakter tylko i wyłącznie techniczny. Mówię o ocenie dostawcy wysokiego ryzyka, nie konkretnego sprzętu i oprogramowania, bo to jest rozwiązanie techniczne. Natomiast jeżeli mówimy czy to o wycofaniu jednego konkretnego dostawcy, czy wielu dostawców, to chcę powiedzieć, że jest to znacząca decyzja i w związku z tym powinna być podejmowana na odpowiednim szczeblu. Chcę też powiedzieć, że w innych państwach, bo cały szereg państw UE w tej chwili albo już wdrożył, albo wdraża mniej więcej podobne rozwiązania bazujące na decyzjach UE, tego typu decyzje podejmowane są na bardzo wysokim szczeblu. Za przykład może posłużyć Francja, gdzie taką decyzję może podjąć premier.

Może jeszcze chwilę poświęcę temu, jak te decyzje są podejmowane w innych państwach, decyzje dotyczące wykluczania dostawców bądź jednego konkretnego dostawcy, bo w kontekście jednego dostawcy rozmawiamy. Chciałbym jeszcze wyraźnie jednak podkreślić, żebyśmy czytali tę ustawę nie jako narzędzie związane z jednym konkretnym dostawcą, żebyśmy oderwali się od kontekstu tylko i wyłącznie jednego dostawcy, tylko spojrzeli na tę ustawę jako narzędzie, które pozwoli nam reagować w sposób legalny w przypadku zaistnienia tego typu zagrożeń także w przyszłości, nie tylko w momencie, kiedy startujemy z budową sieci nowej generacji 5G, ale także w trakcie jej użytkowania. W trakcie użytkowania tej sieci też mogą pojawić się zagrożenia, też mogą pojawić się dostawcy wysokiego ryzyka. Do tego musimy mieć odpowiednie narzędzia. Jest oczywiście kwestią dyskusji to, czy mechanizmy są odpowiednio dobrane. Będziemy o tym dyskutować w trakcie procesu konsultacji, które prowadzimy, i uzgodnień nad projektem ustawy. Bez wątpienia musimy mieć takie mechanizmy, które pozwolą nam odpowiednio zareagować.

Takie mechanizmy wdrożyła już Estonia, o czym mówił m.in. pan poseł. Takie mechanizmy na poziomie prac parlamentarnych wdraża Finlandia, gdzie wśród głównych kryteriów brane jest pod uwagę zagrożenie dla bezpieczeństwa narodowego i obrony

narodowej jako kryterium wykluczające z użytku sprzęt komunikacji elektronicznej. We Francji kryterium ochrony interesów bezpieczeństwa narodowego i obrony państwa jest jednym z podstawowych kryteriów. Jak powiedziałem, decyzję wydaje premier, ale jest ona wydawana na podstawie oceny ryzyka dokonanej pod kątem poziomu zabezpieczenia urządzeń oraz przewidywanego sposobu zabezpieczenia i przewidywanego sposobu rozmieszczania urządzeń, także pod kątem ich użytkowania oraz faktu znajdowania się operatora lub jego usługodawców pod wpływem państwa trzeciego niebędącego państwem członkowskim UE. Znowu jest więc dokładnie czy prawie dokładnie tak, jak jest w naszych przepisach.

W Szwecji przy dokonywaniu oceny ryzyka bierze się pod uwagę wpływ na działalność wnioskodawcy państwa trzeciego oraz państw i organizacji prowadzących ofensywne działania w cyberprzestrzeni. Brana jest pod uwagę także kwestia prawodawstwa państwa wnioskodawcy, szczególnie pod kątem poszanowania zasad praworządności i ochrony danych.

Wielka Brytania jest już poza UE. Działalność operatorów telekomunikacyjnych podlega ocenie pod kątem zagrożenia dla cyberbezpieczeństwa. Narodowe centrum cyberbezpieczeństwa na wniosek rządu może zarekomendować ograniczenia lub wyłączenie działalności dostawcy wysokiego ryzyka.

To tylko kilka państw, które podejmują działania w tej chwili. Niemcy pracują nad swoim projektem ustawy. Ten proces się toczy. Oczywiście są bardzo różne dyskusje, które odnoszą się do konkretnych dostawców, ale mają także charakter obiektywny, dlatego że wszyscy zdają sobie sprawę z tego, jak istotne jest bezpieczeństwo sieci teleinformatycznych.

Była też tutaj mowa o potencjalnych opóźnieniach. Chcę powiedzieć, że nie wiem, skąd wywodzony jest ten argument, dlatego że nie mamy jednego dostawcy sprzętu do budowy sieci 5G na świecie. Tych dostawców jest kilku, z czego dwóch jest europejskich, dwóch bardzo aktywnych w Polsce, także bardzo dużo w Polsce inwestujących. Chcę powiedzieć, że i Ericsson, i Nokia są firmami, które budują sieci. Mówię o firmach prowadzących aktywną działalność w Polsce, zatrudniających w Polsce po kilka tysięcy osób przy pracach badawczo-rozwojowych, inwestujących. W przypadku Ericssona są to inwestycje rzędu 5 mld zł rocznie w działania R&D i w produkcję sprzętu do budowy sieci 5G. Są to firmy, które budują sieci telekomunikacyjne na całym świecie, więc argument o wyłączeniu jakiegokolwiek jednego z dostawców według mnie nie znajduje żadnego uzasadnienia. Przy czym jeszcze raz podkreślam, że w tej chwili nie podejmujemy żadnej decyzji. Podejmujemy decyzje ewentualnie o wypracowaniu sobie odpowiedniego oprzyrządowania do tego, żeby można było odpowiednio reagować.

Była też mowa o ograniczeniu konkurencji. Chcę powiedzieć, że jeśli chodzi o sieci 4G, w Polsce, gdzie – myślę, że jest co do tego pełna zgoda – rynek telekomunikacyjny jest jednym z najbardziej konkurencyjnych w Europie, mamy dostawców, którzy korzystają ze sprzętu Huawei, żeby już wypowiedzieć tę nazwę, ale mamy także takiego operatora telekomunikacyjnego, który nie korzysta w ogóle ze sprzętu Huawei. Mimo wszystko podmioty te konkurują, funkcjonują na tym samym rynku i nie widać, żeby ktoś zyskiwał jakąś specjalną przewagę na skutek tego, że korzysta ze sprzętu takiego bądź innego dostawcy.

Była wreszcie mowa o olbrzymich kosztach, które poniosą telekomunikacyjni operatorzy. Nasza propozycja przewiduje czas na ewentualne wycofanie sprzętu, o ile zostanie wskazany dostawca wysokiego ryzyka. Jeszcze raz to podkreślę – o ile w ogóle zostanie wskazany, bo my tylko tworzymy odpowiedni zestaw narzędzi. Czas, który na to zaproponowaliśmy w przypadku dostawcy wysokiego ryzyka, a który będzie podlegał dyskusji, bo mamy postulat, żeby ten czas wydłużyć, wynosi co najmniej pięć lat, być może siedem lat, tak jak jest w Wielkiej Brytanii. To czas, który powoduje, że proces wycofania jest procesem naturalnym. Wymiana sprzętu i tak następuje w takich cyklach, czasami nawet w szybszych. Analizy jednej z firm konsultingowych wskazują, że w skali całej UE potencjalny koszt związany z wymianą tego sprzętu w związku z przyspieszaniem tego typu procesów to 3,5 mld euro. W przeliczeniu na jednego abonenta jest to

ok. 6,5 euro. Informacja, że w Polsce ma to być kilkanaście miliardów złotych, jest więc niczym niepoparta.

Proszę zwrócić uwagę, że jeden z operatorów powiedział, jakie ewentualnie może ponieść koszty. Bardziej mówił o tym, jakiej wartości sprzęt będzie musiał wymienić. Jest to kwota 900 mln zł. Ta kwota, jeśli podzielimy ją przez siedem lat, to ok. 120 mld zł. Chcę zwrócić uwagę na to, że wydatki marketingowe tylko jednego operatora telekomunikacyjnego to jest ok. 330 mln zł rocznie. Oczywiście może to wiązać się z jakimś kosztem, z całą pewnością nie mówimy tutaj o tym, że będzie się to odbywało całkowicie bezboleśnie. Każda tego typu ingerencja w gospodarkę musi powodować reakcję, natomiast z całą pewnością szacunki, które w tej chwili podawane są w przestrzeni publicznej, to szacunki co najmniej przesadzone. Tym niemniej, tak jak powiedziałem, jesteśmy otwarci na dyskusję nad ostatecznym kształtem tej ustawy. Zapraszamy zresztą i zapraszaliśmy do tej dyskusji wszystkie podmioty. Mamy już bardzo dużo stanowisk, które do nas wpłynęły. Będziemy analizować wszystkie te propozycje.

Kończąc wystąpienie, chciałbym powiedzieć, że cały ten projekt jest odpowiedzią zarówno na konieczność zapewnienia jak najwyższego standardu bezpieczeństwa sieci telekomunikacyjnych, bo jest to niezbędne do sprawnego i bezpiecznego funkcjonowania państwa, ale także jest to odpowiedź na proces, który w tej chwili odbywa się na forum UE i NATO, w którym to procesie Polska od samego początku aktywnie uczestniczy. Rozwiązania, które zostały wypracowane m.in. w ramach „5G toolbox", były rozwiązaniami, w których spory wkład miała m.in. Polska. Bardzo dziękuję.

Przewodniczący poseł Marek Kuchciński (PiS):

Dziękuję panu ministrowi. Proszę państwa, w tej chwili przystąpimy do dyskusji. Zgłosiło się już kilkoro posłów. Według kolejności zgłoszeń… Proponowałbym, żeby najpierw udzielać głosu posłom będącym tu, na sali. Zgłosił się więc poseł Sławomir Nitras, następnie przewodniczący Paweł Zalewski i poseł Jacek Kurzępa. Panie pośle, proszę bardzo.

Poseł Sławomir Nitras (KO):

Dziękuję, panie przewodniczący. Z jednej strony cieszę się, że do tej dyskusji dochodzi, i dziękuję panom ministrom, szczególnie panu ministrowi Zagórskiemu, za wyczerpującą i solidną dawkę wiedzy. Z drugiej strony trochę martwi mnie, że można – mam nadzieję, że mylnie – odnieść wrażenie, że intencją zwołania tego posiedzenia Komisji była chęć występowania w interesie jednego czy tylko części dostawców usług. Tak to może zostać przez niektórych odebrane, a myślę, że warto to wyprostować.

Nie ma dla mnie najmniejszej wątpliwości, że w XXI w. pojęcie, jak wyraził się pan minister, „dostawca wysokiego ryzyka" (pojęcie to nie było mi wcześniej znane), szczególnie jeśli chodzi o infrastrukturę informatyczną czy cyfrową, jest pojęciem kluczowym. Jeżeli żyjemy – a żyjemy – w rzeczywistości, w której struktura przesyłowa, energetyczna czy gazowa jest kluczowa, to w XXI w. infrastruktura cyfrowa jest na pewno tym bardziej kluczowa.

Na pewno ani państwu polskiemu, ani UE, ani NATO dostawca tych usług i kontrola nad ich systemem, brak wpływu państw trzecich na dostęp do tej infrastruktury nie tylko ze względu na bezpieczeństwo państwa, które jest najważniejsze, ale też ze względu na bezpieczeństwo obywateli, na te wartości, które są dla nas najważniejsze, takie jak demokracja, wolność słowa, brak manipulowania opinią publiczną – to są rzeczy absolutnie kluczowe… Z tej perspektywy państwo musi – wydaje mi się, że większość społeczeństwa oczekuje, że państwo w tej materii nie będzie bezsilne. To, jak duży jest to kłopot, pokazują doświadczenia większych i znacznie potężniejszych państw na świecie, łącznie ze Stanami Zjednoczonymi. Co do przyszłości, z kierunkiem określonym przez pana ministra Zagórskiego mogę się tylko zgodzić. Chciałbym tylko zadać kilka pytań.

Mam świadomość miejsca, roli i potencjału polskiego przemysłu w tej materii, ale czy jest szansa, żebyśmy odegrali aktywną rolę w ramach budowy czy to europejskich, czy to transatlantyckich rozwiązań gospodarczych w tym zakresie? Chciałoby się, żebyśmy byli uczestnikiem, a nie tylko odbiorcą tej rewolucji. Bo na naszych oczach odbywa się rewolucja. To jest pierwsze pytanie.

Moje drugie pytanie jest takie. Wspomniał pan o tym, mówiąc o infrastrukturze, która jest dzisiaj. Wiem, że dziś jesteśmy mądrzejsi o doświadczenia ostatnich lat, ale czy ta infrastruktura jest dzisiaj bezpieczna, biorąc pod uwagę to, o czym mówiłem wcześniej, a o czym mówił przede wszystkim pan, czyli to, że nie wszyscy dostawcy usług są bezpieczni? Biorąc pod uwagę to, że – jak pan powiedział – przynajmniej niektórzy dostawcy w dużym zakresie korzystają z takiego sprzętu, czy ta infrastruktura, z której korzystamy, z punktu widzenia interesów państwa i z punktu widzenia zwykłego obywatela jest bezpieczna? Rozumiem, że bardzo dużo mówi się o tym, jak w przyszłości będzie działała infrastruktura 5G czy nawet – jak mówicie panowie – 6G. Co jednak z dotychczasową infrastrukturą? Czy istnieje strategia zabezpieczenia, zastąpienia?

Wiem, że pan mówił o kwotach, tylko jest pytanie, czy umiemy oszacować koszty, czy mamy jakiś pomysł, jak tę infrastrukturę zamienić. Czy jest to kwestia tylko postępu technologicznego i zmiany starej tak, że stara po prostu przestaje być użyteczna? Byłbym zobowiązany, gdyby pan minister był łaskaw powiedzieć w tej sprawie parę słów. Dziękuję uprzejmie.

Przewodniczący poseł Marek Kuchciński (PiS):

Dziękuję bardzo. W tej chwili poproszę o zabranie głosu pana przewodniczącego Pawła Zalewskiego.

Poseł Paweł Zalewski (KO):

Dziękuję bardzo, panie przewodniczący. Dziękuję za zorganizowanie tego posiedzenia i gratuluję panu posłowi Andrzejowi Szejnie, bo uważam, że rzecz jest najwyższej wagi, a do tej pory, przynajmniej w tej kadencji, nie była na posiedzeniach naszej Komisji wystarczająco omawiana.

Warto spojrzeć na kwestie cyberbezpieczeństwa w szerszym kontekście. Jest tak, że świat zaczyna dzielić się na dwa rywalizujące ze sobą bieguny, czyli na Stany Zjednoczone i na Chiny. To jest godne ubolewania, bo czas tej globalnej współpracy już minął. Był bardzo korzystny także dla nas. Wyłania się jednak nowy porządek. W porządku tym Polska musi znaleźć się przede wszystkim w ramach UE.

Rozumiem informacje, które pan minister Wawrzyk i pan minister Zagórski przekazywali, w taki sposób, że naszym pierwszym punktem odniesienia jest współpraca w ramach UE i tworzenie instrumentu bezpieczeństwa technologicznego, a w ramach bezpieczeństwa technologicznego także bezpieczeństwa cybernetycznego w UE, a następnie próba współpracy transatlantyckiej ze Stanami Zjednoczonymi. Uważam, że jest to dobry kierunek, chociaż biorąc pod uwagę politykę pana Trumpa, obecnego prezydenta Stanów Zjednoczonych, mam przekonanie, iż Europa powinna w większym stopniu budować swoją niezależność także wobec różnego rodzaju zmian amerykańskiej polityki, których można spodziewać się w przyszłości. Zawierzenie w technologicznych kwestiach relacjom ze Stanami Zjednoczonymi może być dla nas groźne, stąd uważam, że Polska powinna wpierać te działania UE, które budują suwerenność technologiczną, a w ramach tego suwerenność w zakresie informatyki i cyberbezpieczeństwa. To jest dobry kierunek.

Jeżeli patrzymy na działania Chin, a one, jak rozumiem, są naszym punktem odniesienia, rozumiem, że – jak powiedział pan minister – dzisiaj szukamy ustawowych zabezpieczeń przed wszystkimi potencjalnymi dostawcami czy sprzętem. Nie dotyczy to wyłącznie jednego dostawcy. Wiemy przecież, że firmą, wobec której jest najwięcej zastrzeżeń z punktu widzenia bezpieczeństwa, a która posiada zarazem duże technologiczne możliwości dostawy systemów, w tym systemu 5G, jest chińska firma Huawei.

Musimy więc zastanowić się nad tym, jakie konsekwencje będą dla nas występowały w przypadku zastosowania tych zapisów wobec tej właśnie firmy i wobec koncepcji Chin, które w ramach polityki jednego pasa i drogi tworzą mechanizmy powiązań gospodarczych, które mają zorganizować świat na gospodarkę zdominowaną czy też z dużymi wpływami chińskimi oraz gospodarkę, które tym wpływom się opierają. Taka jest chińska koncepcja i taka jest rola Huawei w tej polityce.

Nie możemy się oszukiwać i nie możemy o tym nie mówić. Musimy wyraźnie sobie powiedzieć, że potencjalne wykorzystanie tych instrumentów, które tworzy UE,

a w ramach UE Polska, doprowadzi do bardzo silnego ograniczenia funkcjonowania Huawei w Polsce. Zresztą i tak myślę, że po działaniach ABW – myślę tu o aresztowaniu osób oskarżonych o szpiegostwo na rzecz Huawei – zdolności ekspansji tej firmy w Polsce zostały ograniczone. Niezależnie od tego w momencie, w którym instrumenty te zostaną wykorzystane… Wszyscy wiemy, jakie są powiązania, a może inaczej – wiemy, jaka jest natura tych powiązań, ale nie znamy szczegółów, więc jest tu kwestia transparentności. Wiemy, jaki rodzaj systemu politycznego w kontekście praworządności i praw obywatelskich ma miejsce w Chinach itd., itd. Wiemy więc, jak się to skończy, jakie będą konsekwencje tego typu działań – które popieram – dla relacji polsko-chińskich.

Polska deklarowała, że jest zaangażowana w realizację chińskiego projektu jednego państwa i jednego szlaku. Projekty infrastrukturalne, które są w Polsce realizowane, przywołam tu Via Carpatia, mają ścisły związek z planami chińskimi, ale także, jak rozumiem, ściśle z tym związane są plany budowy Centralnego Portu Komunikacyjnego, który, jak rozumiem, w zamyśle jego twórców miał stać się hubem łączącym Chiny z UE, stąd jego olbrzymi rozmach. Doceniam wszystkie koncepcje wiążące infrastrukturalnie Polskę, także w kontekście CPK, ale nie oszukujmy się, ekonomiczny sens tego przedsięwzięcia wyrażany jest uczestnictwem Polski w chińskim programie jednego pasa i szlaku, w tworzeniu infrastrukturalnych więzi Chin z Europą, także w rywalizacji ze Stanami Zjednoczonymi, bo przecież to nie tylko Stany Zjednoczone mogły rywalizować o relacje z Europą, ale robią to także Chiny.

W związku z tym pytanie do przedstawicieli rządu jest następujące. Czy panowie nie obawiacie się, że zastosowanie tych – powtarzam: słusznych – założeń, ważnych z punktu widzenia cyberbezpieczeństwa Polski w UE, doprowadzi do schłodzenia relacji polsko-chińskich w taki sposób, że podważy to ekonomiczny sens inwestycji, które są realizowane, a które, przypomnijmy, jeżeli chodzi o CPK, miały być realizowane także z udziałem instrumentów finansowych kontrolowanych przez rząd chiński? Czy rząd nie powinien zawczasu pomyśleć o zmianie strategii istotnej z punktu widzenia rozwoju gospodarczego Polski i dostosowaniu jej do możliwych konsekwencji, tak żeby plany, które realizuje rząd, były realne i żeby odpowiadały także nowym relacjom globalnym, w które wpisana jest Polska? Dziękuję bardzo.

Przewodniczący poseł Marek Kuchciński (PiS):

Dziękuję panu przewodniczącemu. Teraz poproszę o głos pana posła Jacka Kurzępę. Czy jesteśmy na łączach z panem posłem? Jesteśmy. Panie pośle, proszę bardzo.

Poseł Jacek Kurzępa (PiS):

Serdecznie państwa witam. Dziękuję bardzo za dzisiejszą debatę. Wystąpienie i inicjatywę posłów wnioskodawców odczytuję jako wystąpienie w dobrej wierze i z troski zarówno o transparentność decyzji dotyczących wdrażania nowoczesnych technologii w Polsce, jak i z troski o interes Polski w tym zakresie. Dlatego też wystąpienia obu panów ministrów, zarówno pana ministra Piotra Wawrzyka, jak i Marka Zagórskiego, odczytuję i uznaję za klarowne, pełnowymiarowe, otwarte na wyartykułowane przez wnioskodawców niepokoje. Jednocześnie chciałbym wnieść dwie, trzy refleksje w tej debacie.

Rzeczywiście jesteśmy w czasie przełomowych zmian technologicznych, których Lemowska czy Tofflerowska wyobraźnia nie ogarniała w taki sposób, w jaki doświadczamy ich dzisiaj. Najbliżej tego scenariusza jest Manuel Castells z jego „Galaktyką internetu". Dziękuję, panie ministrze Piotrze Wawrzyk, za przywołanie przewidywanych konsekwencji gospodarczych, ekonomicznych, ale również związanych z rynkiem pracy, których owocem ma być wdrażanie technologii 5G czy 6G.

W pana refleksji pojawia się równocześnie bardzo pożądany nurt pokazujący konieczność współpracy międzynarodowej w tym zakresie i dokonania, które w ostatnim czasie są udziałem zarówno pana resortu, jak i resortu pana ministra Marka Zagórskiego. Myślę o konferencji praskiej, myślę o porozumieniach polsko-amerykańskich, myślę również o rozmowach z naszymi partnerami z Chin. Nie zmienia to postaci rzeczy, że konieczna współpraca międzynarodowa jest osadzona przede wszystkim w synergii i dialogu z poli-

tyką UE, o której obaj ministrowie mówiliście bardzo wyraźnie, pokazując faktografię dokonań obu ministerstw.

Druga rzecz jest taka, że prócz współpracy i dialogu międzynarodowego w tym zakresie naturalną i oczywistą rzeczą jest międzynarodowa rywalizacja o miejsce w peletonie zmian i wytyczenie drogi, która w naszej perspektywie przede wszystkim byłaby naznaczona dbałością o interes Polski, zarówno ekonomiczny, w gospodarce, jak i interes związany z bezpieczeństwem. Dlatego też to, co zostało przez panów ministrów wyartykułowane, a mianowicie osadzenie perspektywy dbałości o interes polski w trzech aspektach: bezpieczeństwa, które rozpisuje się na bezpieczeństwo danych, bezpieczeństwo użytkowników… Tu jest jedno z pytań, które chciałbym wyartykułować, gdyż naszej debacie z pewnością przysłuchuje się wielu naszych współobywateli, których troska skupiona jest w dużym stopniu na pytaniu o bezpieczeństwo użytkownika, o to, czy te technologie nie są technologiami, które w jakiejś mierze mogą grozić czy to środowisku i otoczeniu, czy zdrowiu i życiu użytkownika. W tej perspektywie bezpieczeństwa mówimy również o kwestii cyberbezpieczeństwa. Dlatego, panie ministrze Marku Zagórski, to, że rozważamy kwestię powołania Kolegium ds. Cyberbezpieczeństwa i uplasowanie pana premiera jako najwyższej rangi reprezentanta gremium decyzyjnego, uznaję za zasadne ze względu na sprawę, o jakiej w tej chwili debatujemy, i istotną, newralgiczną kwestię dotyczącą właśnie cyberbezpieczeństwa naszego kraju.

W wytycznych, które przedstawił pan minister Zagórski, mówimy o bezpieczeństwie ocenianym zarówno według naszego własnego pomiarowania według kryteriów wewnątrzkrajowych, jak i wychodząc naprzeciw oczekiwaniom UE i oceniając zarówno dostawcę, jak i konkretny sprzętu oraz konkretne oprogramowanie. Pan minister podkreśla to zróżnicowanie. Dziękuję za tę wrażliwość i troskę, a przywołując jednocześnie pewne modelowe rozwiązania, czy to estońskie, czy francuskie, czy szwedzkie, czy brytyjskie, wydaje się, że usytuowanie poziomu decyzyjnego w rękach kolegium i pana premiera jest adekwatne i synergiczne do tego, co dzieje się w perspektywie europejskiej.

Reasumując, chciałbym serdecznie za tę debatę podziękować. Jest ona przede wszystkim merytoryczna. Troska koleżeństwa z opozycji jest uzasadniona. Wystąpienia obu ministrów jeszcze raz oceniam jako bardzo merytoryczne, bardzo soczyste, bogate w faktografię i wyjaśniające zawiłości międzynarodowych relacji w globalnym wyścigu technologii cyfrowej. Dziękuję bardzo.

Przewodniczący poseł Marek Kuchciński (PiS):

Dziękuję panu posłowi. Szanowna Komisjo, więcej zgłoszeń państwa posłów nie widzę. Informuję, że o głos prosiło jeszcze troje przedstawicieli, którzy zostali zgłoszeni przez pana posła Szejnę jako eksperci i których zaprosiłem do udziału w posiedzeniu Komisji. Jest to pani Agnieszka Maliszewska, sekretarz i dyrektor biura Polskiej Izby Mleka, pan prof. Edward Haliżak z Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego oraz pan Stefan Kamiński, prezes Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji. W takiej kolejności prosiłbym państwa o zabranie głosu. Bo jak rozumiem, zgłosili państwo chęć zabrania głosu.

Proszę, pani Agnieszka Maliszewska. Jeszcze raz przypomnę, że pani Agnieszka Maliszewska jest sekretarzem i dyrektorem biura Polskiej Izby Mleka. Czy mamy kontakt? To może zaczekamy, a w tej chwili o zabranie głosu poproszę pana prof. Edwarda Haliżaka. Dzień dobry, proszę bardzo.

Profesor na Wydziale Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego Marian Edward Haliżak:

Dzień dobry państwu. Zostałem przez posła Szejnę poproszony o wyłożenie krótkiej opinii o stosunkach Polska–Chiny, ponieważ tematem tym zajmuję się od wielu lat. Z dużym zainteresowaniem wysłuchałem wystąpień przedstawicieli rządu, którzy w kontekście bezpieczeństwa posługują się terminem „dostawca wysokiego ryzyka”. To taki fajny eufemizm, ponieważ mówiąc „dostawca wysokiego ryzyka”, wszyscy myślą o chińskiej firmie Huawei. Takie mamy czasy.

Zgadzam się z posłem Zalewskim co do tego, że wchodzimy w erę dwubiegunowości między Chinami a Stanami Zjednoczonymi. Wszystkie kwestie, o których państwo dys-

kutowaliście, są funkcją stosunków USA–Chiny i stosunków Polska–USA. Dla naszego kraju w imię własnej racji stanu wszystkie kwestie związane z bezpieczeństwem i współpracą z Chinami musimy starannie wyważyć.

Wiele jest płaszczyzn współpracy polsko-chińskiej. Ja reprezentuję branżę, która świadczy usługi edukacyjne dla Chin rozumiane jako oferta studiów w języku angielskim dla studentów z Chin na kierunku stosunki międzynarodowe. W tym roku zrekrutowaliśmy grupę ponad 30 studentów z Chin. W sumie mamy ponad 50 osób. W całym Uniwersytecie Warszawskim to jest ponad 200 osób na różnych wydziałach. Uważam, że polskie uczelnie są bardzo dobrym miejscem studiowania dla chińskiej młodzieży. W ocenie edukacyjnych władz chińskich postrzeganie Polski jako miejsca studiowania dla chińskiej młodzieży jest bardzo wysokie ze względu na przyjazny Chinom kontekst.

Odnosząc się do kwestii bezpieczeństwa w cyberprzestrzeni – rzeczywiście, wkrótce świat będzie podzielony na cyberprzestrzeń chińską i amerykańską. Pozostałe państwa będą miały wybór, do której z nich się przyłączyć. Będzie to wybór podobny do tego, który miał miejsce w czasach zimnej wojny: albo Związek Radziecki, albo Zachód z USA. Ten dylemat miały państwa Trzeciego Świata. W tej sprawie Polska będzie musiała po prostu wybrać. Różnica polega jednak na tym, że mamy parę dziedzin współpracy z Chinami, które warto byłoby zatrzymać.

Na koniec chciałbym powiedzieć, że jest jeszcze jeden element, który nasze stanowisko wobec Chin będzie bardzo silnie determinował, mianowicie perspektywa podpisania do końca tego roku bilateralnej umowy o inwestycjach między UE a Chinami. Wedle wszelkich nowszych informacji prace w tej dziedzinie są bardzo zaawansowane i jeżeli taka umowa zostanie podpisana, będzie to miało przełożenie na wszystkie projekty inwestycyjne realizowane między Chinami a Polską. Wtedy oczywiście otworzą się zupełnie inne perspektywy.

W moim przekonaniu jako Polska, jako kraj stoimy przed jednoznacznym wyborem: albo Stany Zjednoczone, albo Chiny. W związku z tym sytuacja rzeczywiście jest bardzo istotna z punktu widzenia decyzyjnego celów krótkofalowych i celów długofalowych. W tej bardzo specyficznej płaszczyźnie do pewnego stopnia jesteśmy świadkami powrotu do zimnej wojny. Dziękuję.

Przewodniczący poseł Marek Kuchciński (PiS):

Dziękuję panu profesorowi. Czy z panią Agnieszką Maliszewską jesteśmy na łączach? Witam panią. Dzień dobry. Proszę o zabranie głosu.

Sekretarz, dyrektor biura Polskiej Izby Mleka Agnieszka Maliszewska:

Panie przewodniczący, panowie ministrowie, panie i panowie posłowie, bardzo dziękuję za zaproszenie. Postaram się bardzo szybko odnieść się do kilku kwestii. Dziękuję bardzo za tę debatę, ponieważ jest niezwykle istotna z punktu widzenia przyszłości chociażby sektora, który reprezentuję. Reprezentuję sektor mleczarski, ale nie tylko, bo jestem też wiceprezydentem COGECA. Jest to największa w Europie organizacja zrzeszająca spółdzielców, różnych przetwórców i różne spółdzielnie całego sektora rolno-spożywczego. Dzisiejsza debata i dzisiejsza dyskusja jest niezwykle istotna także z punktu widzenia naszej branży.

Niezwykle ważne jest to, o czym mówił pan minister Zagórski, czyli kwestia w szczególności związana z naszym bezpieczeństwem, z bezpieczeństwem kraju. Chyba wszyscy musimy mieć też świadomość – i prawdopodobnie taką świadomość mamy – że od momentu, kiedy pierwszy raz zaczęliśmy używać smartfonów, które dzisiaj towarzyszą nam codziennie, nasza anonimowość, a trochę nasze bezpieczeństwo obywatelskie nie jest już na takim poziomie, na jakim było kiedyś.

Wszystkie kwestie związane z dyskusją na temat niezwykle dziś istotny, przynajmniej moim zdaniem, zdaniem eksperta sektora mleczarskiego i osoby, która od wielu lat pracuje m.in. na rynku chińskim, po to, by wzmocnić eksport polskich – i nie tylko polskich, ale też europejskich – produktów, i mleczarskich, i rolno-spożywczych, na ten rynek, warto by przy tej dyskusji wziąć pod uwagę także aspekt ekonomiczny, o którym mówił pan poseł Zalewski.

Dziś oczywiście mamy świadomość tego, że rozmawiamy o dwóch najważniejszych graczach, jeżeli chodzi o kwestię dostawy całego systemu 5G. Natomiast w punktu widzenia nas, czyli rolników, przetwórców, eksporterów, istotne jest, abyśmy w tej dyskusji nie pominęli kwestii związanej z niezwykle istotną sprawą związaną z gospodarką, z naszymi rynkami zbytu, z naszymi odbiorcami, także tymi, którzy są dziś naszymi bardzo strategicznymi partnerami, z którymi prawdopodobnie – mamy taką nadzieję – będziemy współpracować przez wiele lat. To m.in. po to tworzony był ten szlak, o którym wspominał pan poseł Zalewski. Prośba jest więc taka, by w dyskusjach pamiętać o tym, że kwestia związana z gospodarką i z ekonomią jest elementem, który też powinien być brany pod uwagę. Dziękuję uprzejmie.

Przewodniczący poseł Marek Kuchciński (PiS):

Bardzo pani przewodniczącej dziękuję. W tej chwili mam zgłoszonego do głosu pana Kamińskiego, prezesa Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji. Czy jesteśmy w kontakcie na łączach? Czy mamy kontakt z panem Stefanem Kamińskim? Wyłączył się.

Proszę państwa, po wyczerpaniu mówców w dyskusji poprosiłbym panów ministrów o odniesienie się do zgłoszonych zagadnień i o odpowiedzi na pytania, bo został sformułowany cały szereg pytań.

Nie mam kontaktu z panem Kamińskim. W takim razie za udział dziękuję wszystkim państwu, którzy zabrali głos w dyskusji. Który z panów ministrów pierwszy? Pan minister Wawrzyk pierwszy zabierze głos. Proszę bardzo.

Sekretarz stanu w MSZ Piotr Wawrzyk:

Panie przewodniczący, dziękuję bardzo. Wysoka Komisjo, bardzo dziękuję za wszystkie głosy. Chciałbym odnieść się do tego najważniejszego wątku, który pojawił się w kilku wystąpieniach, mianowicie do sformułowania odwołującego się do jednej z firm chińskich i ewentualnego wpływu na relacje polsko-chińskie, gdyby okazało się, że założenia ustawy, którą prezentował pan minister Zagórski, mogą mieć taki wpływ.

Chciałbym zwrócić uwagę na dwa aspekty. Po pierwsze, relacje te są wielopłaszczyznowe. Tak jak wspominał pan prof. Haliżak, nie jest to tylko kwestia technologii 5G. To jest kwestia współpracy edukacyjnej, to jest kwestia, tak jak mówiła pani przewodnicząca, współpracy towarowej, ale oczywiście to jest też kwestia CPK. Przy czym zwracam uwagę, że w tym ostatnim wymiarze jest to kwestia dwustronnych korzyści. To nie jest tak, że budujemy CPK i tylko my czy Chińczycy będziemy mieli z tego korzyść, ale korzyść będzie z tego miała cała Europa, bo celem CPK nie jest stworzenie centrum dystrybucji artykułów chińskich na Polskę, ale na Europę.

W tym wymiarze jest to zbyt szeroki problem, aby taka kwestia jak 5G mogła w jakiś sposób na niego rzutować. Zwracam uwagę, że technologia 5G jest tylko jednym z aspektów relacji polsko-chińskich czy szerzej – europejsko-chińskich. W tym kontekście przypominam też to, o czym szerzej powie pewnie pan minister Zagórski. Nasze regulacje proponowane w tym zakresie w niczym nie odstają od zaleceń ustalonych na poziomie europejskim i od tych, które są przyjęte przez inne państwa europejskie. Nie można więc na to patrzeć wyłącznie z perspektywy relacji bilateralnych z Chińską Republiką Ludową. Dziękuję bardzo.

Przewodniczący poseł Marek Kuchciński (PiS):

Dziękuję bardzo. Proszę o zabranie głosu pana ministra Marka Zagórskiego.

Sekretarz stanu w KPRM Marek Zagórski:

Panie przewodniczący, szanowni państwo, pytań było całkiem sporo. Zacznę może od wątku dotyczącego współpracy i relacji z Chińską Republiką Ludową wykraczających poza 5G, ale związanych z obszarem technologii cyfrowych.

Dialog z władzami chińskimi prowadzimy w dużo szerszym zakresie, wykraczającym bardzo mocno poza 5G. Mamy opracowaną specjalną agendę polsko-chińskich konsultacji cyfrowych. Obejmuje ona cały szereg zagadnień: od gospodarki cyfrowej, poprzez rozwój nowych technologii, takich jak sztuczna inteligencja, ale także ochrona przepływu danych osobowych, zarządzanie internetem, również w kontekście tego, że Polska

jest planowana jako gospodarz Światowego Forum Zarządzania Internetem. Miało to się odbyć w tym roku, ale z powodu pandemii jest przeniesione na rok przyszły.

Zaproponowaliśmy podpisanie przez polskie instytucje z odpowiednikami chińskimi m.in. trzech memorandów, także w obszarze cyfrowym. To wszystko się dzieje. Są też kwestie bezpieczeństwa sieci, poszczególnych dostawców. Staramy się traktować to odrębnie. Oczywiście nie da się tego traktować całkowicie odrębnie, jednak staramy się traktować to w miarę możliwości niezależnie i nie zakłócać dobrych relacji, które w niektórych obszarach mamy tradycyjnie. Są to m.in. te obszary, o których wspominała pani Agnieszka Maliszewska.

Chcę dla równowagi przypomnieć – a związane z rolnictwem tematy pani sekretarz doskonale zna, mi też są skądinąd znane – że jeżeli chodzi na przykład o mięso wieprzowe, mamy zakaz importu od 13 lutego 2014 r. Przez długotrwałe procedury administracyjne nie jesteśmy w stanie z jakimkolwiek sukcesem ulokować mięsa wołowego. Jeśli chodzi o mąkę, to procedura zatwierdzająca wniosek trwa od 2016 r. Jeżeli chodzi o owoce świeże, trwa to od 2017 r., jeżeli chodzi o mrożone owoce, to też trwa to od 2017 r. Relacje te oczywiście więc są, ale trzeba pamiętać, że problemy pojawiają się po obu stronach i nie możemy zapominać o tym także w kontekście rozmowy o konkretnej technologii.

Przechodząc do kwestii technologicznych i jeszcze nawiązując do pytań pana posła Nitrasa w szerszym wymiarze dotyczących bezpieczeństwa, bo było pytanie o to, czy w związku z tym, że mamy sieci 4G, które wykorzystują infrastrukturę tego konkretnego podmiotu, jesteśmy bezpieczni i jak to się ma do bezpieczeństwa generalnie, trzeba najpierw powiedzieć o specyfice technologii 5G i o tym, o czym tak naprawdę mówimy, dlaczego jest tak ważna i dlaczego dyskusja ta zaczęła się kilka lat temu.

Przede wszystkim ważna jest dlatego, że mówimy o technologii transferu danych. Mówimy także o tym w kontekście gospodarki opartej na danych. Sieć 5G jest tak istotna dlatego, że pozwala na dużo większy transfer danych niż ten, z którym mieliśmy do czynienia w sieciach poprzedniej generacji. W związku z tym, biorąc też pod uwagę kierunek rozwoju gospodarki, sposób wykorzystania danych przez poszczególne sektory gospodarki i uzależnienie od transferu danych, także transferu danych z wykorzystaniem technologii mobilnych, potrzeba zapewnienia bezpieczeństwa sieci jest dużo większa, niż to było wcześniej.

Nie znaczy to oczywiście, że wcześniej potrzeby bezpieczeństwa nie było. Dotychczas jednak, choć to się nadal nie zmienia, pełną odpowiedzialność za bezpieczeństwo i integralność sieci brali na siebie operatorzy telekomunikacyjni, którzy patrzyli na to z perspektywy zapewnienia bezpieczeństwa swoim klientom. To był ten podstawowy element. W kontekście tego, jak ważny staje się transfer danych, wychodzimy poza kwestie związane z bezpieczeństwem klientów i konsumentów i wchodzimy w dużo szerszy obszar bezpieczeństwa funkcjonowania poszczególnych sektorów gospodarki, wręcz bezpieczeństwa państwa.

Z tego powodu nacisk na bezpieczeństwo sieci 5G jest dużo większy, niż to było w przypadku poprzednich technologii. Trzeba jednak powiedzieć, że sieć 5G, o której teraz mówimy, jest budowana w technologii non-standalone, czyli wykorzystującej dotychczasową infrastrukturę. W pewnym – dużym – zakresie dotychczas wykorzystywane komponenty będą wpływały także na bezpieczeństwo sieci. We wszystkich przypadkach, o których rozmawiamy, mówimy raczej o przyszłości, czyli przy ewentualnym wykluczeniu jakiegokolwiek dostawcy, czy to ma miejsce w Polsce, czy miałoby mieć miejsce w innych państwach, na przykład w Wielkiej Brytanii, mówimy o pięcio- i siedmioletnich terminach pozwalających na tzw. naturalny rollout urządzeń, czyli na zastąpienie urządzeń dostawcy wysokiego ryzyka urządzeniami innych dostawców.

Pytanie, czy jest szansa, byśmy odgrywali w tym procesie rolę na poziomie międzynarodowym. Pan minister Wawrzyk mówił, że żadne państwo w tym obszarze ani nie jest w stanie zapewnić sobie poczucia bezpieczeństwa, ani też samo nie jest w stanie stworzyć rozwiązań, dzięki którym mogłoby zrezygnować z jakiejkolwiek kooperacji. Dzisiaj na jednym z portali zajmujących się technologiami był opis tego, z czego składa się stacja bazowa. Składa się oczywiście z wielu urządzeń chińskich, ale przede wszystkim w 40%

składa się z urządzeń dostarczanych przez podmioty amerykańskie. Bez tych urządzeń stacja bazowa nie mogłaby funkcjonować, po prostu by nie działała. Mówię o tym w kontekście tego pytania – rzeczą naturalną w procesie rozwoju nowoczesnych technologii jest kooperacja. Chcemy kooperować, przede wszystkim koncentrując się na naszych partnerach. Swego czasu pozwoliłem sobie zaproponować takie określenie: oprócz sojuszu politycznego, oprócz sojuszu militarnego istnieje także potrzeba zawarcia sojuszu technologicznego, który wyglądałby troszeczkę inaczej w odniesieniu przede wszystkim do naszych partnerów, tzn. istnieje potrzeba, żebyśmy pracowali nad rozwiązaniami wspólnie. Nie czas teraz rozwijać, na czym miałoby to polegać, jednak w interesie Polski jest współpraca z partnerami w taki sposób, żebyśmy nie byli tylko odbiorcą technologii. To powinno być i jest kluczowym elementem naszej polityki gospodarczej w obszarze nowych technologii.

Chciałem podkreślić, że mamy pełną zgodę z wypowiedzią pana Zalewskiego, który mówił, że musimy zastanowić się, jakie konsekwencje będzie miało zastosowanie mechanizmów europejskich wobec Huawei i wobec Chin, mając na względzie to, o czym mówił pan przewodniczący, że wiele firm, w tym Huawei, jest narzędziem polityki chińskiej. Z całą pewnością jest to brane pod uwagę nie tylko przez nas, w Polsce, ale także w UE, także w kontekście planowanego podpisania porozumienia UE i Stanów Zjednoczonych.

W kontekście technologii 5G cały czas powtarza się pytanie dotyczące bezpieczeństwa. O to pytał pan poseł Jacek Kurzępa. Chcę powiedzieć, że mówimy o różnych poziomach i kwestiach w zakresie bezpieczeństwa. Jest zakres, o którym mówiliśmy wcześniej, czyli cyberbezpieczeństwo sieci. Jest także wymiar bezpieczeństwa, o którym mówią różne środowiska wskazujące na to, że technologia 5G może grozić środowisku, człowiekowi. Chcę podsumować to tylko jednym sformułowaniem, takim, że w tym aspekcie technologia 5G niczym nie różni się od poprzednich technologii, 4G czy 5G, dlatego że wykorzystuje fale radiowe i jej potencjalny negatywny wpływ na środowisko czy na człowieka w żaden sposób nie pogarsza się i nie zwiększa się. Mówię o negatywnym wpływie w tym sensie, że tak naprawdę go nie zaobserwowano. Jeżeli ktokolwiek uważa, że coś się tutaj miałoby pogorszyć, to nie ma żadnego nowego powodu ani czynnika, który pojawiałby się w kontekście technologii 5G. Można nawet powiedzieć, że odwrotnie, zastosowanie tej technologii, moc urządzeń, z których korzystają użytkownicy, jest mniejsza, a tym samym mniejsze jest potencjalne oddziaływanie na pole elektromagnetyczne.

Kończąc i nawiązując do wypowiedzi prof. Haliżaka, który mówił, że czeka nas era podzielonego internetu, chcę powiedzieć, że zauważamy to dopiero z perspektywy europejskiej. Pamiętajmy natomiast, że m.in. w Chinach internet jest podzielony od dawna. Z perspektywy europejskiej mówimy o światowym wolnym internecie. Wolnego internetu nie ma we wszystkich państwach świata – nie wszystkie aplikacje są dostępne, nie wszystkie media społecznościowe funkcjonują. Nie jest to problem, który pojawił się teraz, ale kilka lat temu. Musimy pamiętać także o tym, że nie jest to zjawisko, które objawiło się teraz, aczkolwiek z uwagi na to, jak mocno jesteśmy zanurzeni w świecie cyfrowym, jak bardzo uzależniona od elektronicznego obrotu staje się światowa gospodarka, z całą pewnością wszystkie aspekty związane z ograniczeniami funkcjonowania sieci, z ograniczeniami związanymi z dopuszczaniem na rynek poszczególnych aplikacji i poszczególnych rodzajów oprogramowania będą miały większy wpływ.

Dziękując za możliwość przedstawienia racji z naszej strony i dziękując za to spotkanie, chcę powiedzieć, że z naszej perspektywy wiele tych aspektów jest bardzo istotnych, ale kwestie bezpieczeństwa są i zawsze będą priorytetowe. Dziękuję bardzo.

Przewodniczący poseł Marek Kuchciński (PiS):

Dziękuję panu ministrowi. Proszę państwa, otrzymałem informację, że z panem Stefanem Kamińskim, prezesem Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji, mamy jednak kontakt. Biorąc pod uwagę, że mówimy w kontekście nowych technologii, może jednak warto byłoby połączyć się z panem Kamińskim. Poproszę go o zabranie głosu.

Prezes Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji Stefan Kamiński:

Panie przewodniczący, panie i panowie posłowie, panowie ministrowie, chciałbym powiedzieć, że w stu procentach zgadzam się z tym, co powiedział pan minister Zagórski, jeśli chodzi o kwestie cyberbezpieczeństwa i bezpieczeństwa z tym związanego. Nasza różnica jest tylko taka, że jak to zawsze mówią – diabeł tkwi w szczegółach.

Jako izba przygotowaliśmy 27 stron uwag do propozycji, które dotyczyły zarówno ustawy o KSC, jak i ustawy o zamówieniach publicznych. Chcę tylko podkreślić, że sieć 5G przede wszystkim dedykowana jest – i stąd tak ważna jest kwestia cyberbezpieczeństwa – komunikacji między maszynami, a dopiero w drugiej kolejności nam jako użytkownikom końcowym, ponieważ będzie służyła tym rewolucjom, które są określone m. in. jako przemysł 4.0 czy też Green Deal, czyli możliwościom stworzenia inteligentnych sieci energetycznych. Stąd kwestia budowy tej sieci i jej zabezpieczenia jest bardzo ważna dla każdego kraju, nie tylko dla naszego, ale dla każdego, który myśli o bezpieczeństwie swoich obywateli, ponieważ energia też ma wpływ na bezpieczeństwo nas jako obywateli.

Zwróciliśmy też uwagę na kwestię pewnych zapisów, które naszym zdaniem naruszają pewne obowiązujące przepisy. Reprezentując też operatorów telekomunikacyjnych, obawiamy się, że zapisy narzucone w propozycjach tych ustaw naruszą zapisy wynikające z naszej konstytucji oraz wprowadzą pewną dwuznaczność dotyczącą całej zasady pracy kolegium, o którym mówi się w tej ustawie, mianowicie zasady o przyznaniu pewnych kompetencji, które – przynajmniej zdaniem naszych prawników – nie mają odzwierciedlenia w istniejącym prawie.

Co do kwestii, które były poruszane przez pana posła Zalewskiego, jak kwestia trasy, czy przez pana Kurzępę – kwestię bezpieczeństwa trzeba rozróżniać na dwóch poziomach: z poziomu obywatela oraz z poziomu państwa i jego infrastruktury krytycznej. Chcielibyśmy, żeby operatorzy telekomunikacyjni, którzy w większości są dzisiaj prywatni, bez specjalnych dodatkowych kosztów mogli dostosować się do cyberbezpieczeństwa. Dlatego uważaliśmy, że tym, co powinno być zapisane w projekcie ustawy, jest kwestia powołania się na normy techniczne.

Abstrahując od kwestii wpływania na stosunki międzynarodowe, które zostawiamy innym, bardziej kompetentnym osobom, bo nie jesteśmy politykami, dla nas, z naszego punktu widzenia, czyli z punktu widzenia zarówno dostawców, tych, którzy będą te sieci budowali, jak i użytkowników, ważne są pewne zapisy techniczne, abyśmy nie zostali zmuszeni do wymiany naszych sieci i ponoszenia związanych z tym kosztów. W kwestii dostawców, których rzeczywiście nie ma zbyt dużo, ale są – nie chcielibyśmy, żeby niezbyt jasnymi jeszcze kryteriami, które są zapisane w projekcie ustawy, ograniczyć krąg tych dostawców.

Tym, co jest ważne i co bardzo chciałbym podkreślić, jest to, że chcielibyśmy, żeby uwagi, które napisaliśmy na 27 stronach – trudno, żebym w tej chwili odnosił się do każdego z tych punktów, ale myślę, że one zostaną uważnie przeczytane i w końcowym projekcie czy pracach nad kodeksem cyberbezpieczeństwa zostaną uwzględnione. Dziękuję.

Przewodniczący poseł Marek Kuchciński (PiS):

Bardzo panu dziękuję. Myślę, że w tej chwili możemy już chyba kończyć. Głos pana Stefana Kamińskiego w gruncie rzeczy dotyczył przygotowywanego projektu ustawy i mogę odebrać ten głos w pewnym sensie jako zapowiedź, że tematyka zaproponowana przez pana posła Szejnę z grupą posłów będzie jeszcze kontynuowana na różnych następnych posiedzeniach Komisji nie tylko ze względu na potrzebę sojuszu technologicznego i dyplomacji ekonomicznej, ale także ze względu na to, że – tak jak powiedział pan minister – rewolucja technologiczna bez przerwy trwa i musimy, powinniśmy ją obserwować i pochylać się nad nią w różnych refleksjach. Nad projektem nowelizacji ustawy o systemie bezpieczeństwa cybernetycznego będziemy zapewne pracować w przyszłości.

Proszę państwa, dziękuję panom ministrom i państwu posłom oraz zaproszonym gościom za dzisiejsze spotkanie i dyskusję. Informuję, że na tym porządek obrad został wyczerpany. Protokół dzisiejszego posiedzenia zostanie wyłożony do przejrzenia w sekretariacie Komisji. Zamykam posiedzenie Komisji. Dziękuję bardzo.